**IT Applications, Unit 4**

**Ch 8, Security and Ethical Considerations**

**Disaster Recovery Strategies, p 514**

1. What is a disaster recovery plan?

The disaster recovery plan is a document that tells an organisation what steps are needed to restore the company operations, including computing, in the event of a disaster.

**Preparing a disaster recovery plan:**

1. List some considerations required in preparing a disaster recovery plan.

* Store passwords in two separate secure locations, one of which is in the same building; the second location might be offsite.
* Document the whole recovery process including the location of systems recovery disks. Make sure that all key staff members are familiar with the disaster recovery plan.
* Establish an automated system to notify key staff members of failure in the system. These staff member should be able to know how to start implementing the disaster recovery plan.
* Practice the disaster recovery plan on a quarterly basis. Ensure that new staff understand the process and that all staff are kept up data with new equipment or software.
* Make sure that your backup system works and occurs regularly.
* Build redundancy into your system to eliminate as many points of failure as possible
* Ensure that you have replacement equipment.
* As part of the archive strategy, replace tapes used for back up every 6-9 months
* Buy the best UPS that you can afford
* Protect yourself from theft and employee malice. Ensure data server room is always locked.
* Automatically closing fire doors will keep fire and smoke out of the room. Most disaster recovery plans fail because of lack of backups, practice or documentation.

There are four key parts to a disaster recovery plan:

1. Preparing an emergency plan
   1. What should an emergency plan contain?

* Names and contact details of people to notify, including management and emergency services.
* Procedures to follow with the computer equipment, such as equipment shutdown or removal of files.
* Evacuation procedures for employees, including removal of backup tapes or equipment.
* Return procedures detailing who re-enter the facility and under what circumstances.
* Details of equipment suppliers and insurance providers so that the information system can be rebuilt as quickly as possible.

1. Preparing a “backup” plan
   1. What does a backup plan involve?

An emergency plan explains specific step to be taken in the event of a natural disaster.

* 1. List what the plan should include
* The location of alternative sites and equipment in case the normal computer facility has been destroyed
* The location of backup data, supplies and equipment
* The personnel responsible for gathering backup resources and transporting them to the alternative computing facility
* A schedule indicating the order and approximate time in which each application should be up and running.

1. Preparing a recovery plan
   1. What does a recovery plan involved?

A recovery plan includes specific procedures for restoring the full information processing capacity of the organisation.

* 1. What are the things to consider when writing a recovery plan?
* Identification of mission-critical ICT services
* Use of a backup site for data-processing needs until the primary site has been restored

1. Test plan
   1. What is looked for in testing a disaster recovery strategy?

It is imporatant that an organisation is confident that its data recovery plan will work if needed. For this reason, every part must be fully tested.

**Evaluating information-management strategies,** p 517

Elaborate on each of the following four criteria to consider in evaluating information-management strategies:

1. integrity of data

Data integrity depends on its accuracy, reliability and timeliness.

1. Security

Audit trails and log files can alert you to any problems with logon or file access procedures. You need to be certain that the system is hacker-proof

1. ease of retrieval

Ease of retrieval refers to how easy a file is to find once it has been stored or archived. To achieve this proper file naming conventions should be followed, if they are not followed or are too difficult many files can be ‘lost’ or take long amounts of time to find. Also to ensure files can be easily opened the right file extensions are necessary (if they are wrong the program may not recognise it and will be unable to open it). Correct naming procedures will also assist the organisation in restoring data within the timeframe of the organisation. Organisations and individuals should also be sure to keep logs of where data has been archived, this will allow for easy retrieval in the case of restoring data.

1. currency of files

Files need to be backed-up regularly to ensure that the most recent versions of files are available if needed. If there is a disaster and the backup files are needed to restore the system an organisation can determine how much data has been lost (between backups) and whether or not this amount is.